UNITED STATES DISTRICT COURT

for the
Western District of Arkansas
Fayetteville Division

In the Matter of the Search of Electronic evidence currently in custody of Benton County Sheriff's Office at 1300 SW 14th Street, Bentonville, Arkansas 72712, further described in Application A	)	Case No. 5:19-cm-101

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: **Electronic evidence currently in custody of Benton County Sheriff's Office at 1300 SW 14th Street, Bentonville, Arkansas 72712, more particularly described on "Attachment A".**

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: **See "Attachment B"**

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ■ evidence of a crime;
- ■ contraband, fruits of crime, or other items illegally possessed;
- ■ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)	Distribution, Receipt and Possession of Child Pornography

The application is based on these facts: **See Affidavit of Special Agent Ivan Martinez- "Attachment C"**

■ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Ivan Martinez, Special Agent, Office of the Inspector General
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/19/19

Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, Chief United States Magistrate Judge
Printed name and title

ATTACHMENT A

I am submitting this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to seize and examine digital devices and other electronic storage media, also referred to as "SUBJECT ITEMS" (more fully specified in Attachment A). On August 1, 2019, the SUBJECT ITEMS were seized from the residence located at 17980 Crestwood Drive, Siloam Springs, Arkansas and from the person of Jon Jason Anderson, pursuant to a search warrant issued on July 31, 2019, by the Honorable Robin Green, Circuit Judge for Benton County, Arkansas. This warrant authorizes the seizure of the SUBJECT ITEMS, now being stored as evidence at the Benton County, Arkansas Sheriff's Office, Bentonville, Arkansas, and authorizes a forensic examination of those digital devices (SUBJECT ITEMS), for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(1), (a)(2) and (a)(4)

The below items were taken from the person of Jon Jason Anderson and the residence of Jon Jason Anderson, XXXXX Crestwood Drive, Siloam Springs, Arkansas, pursuant to a search warrant authorized by the Honorable Robin Green, Circuit Court Judge, Nineteenth Judicial Circuit Court of Benton County, Arkansas. Said search warrant authorized the seizure of the electronic devices, which are presently located at the Benton County Sheriff's Office, Bentonville, Arkansas:

1) White Motorola Phone (IMEI: 355569090702296)

2) White Google Pixel Phone (IMEI: 359677093294082)

3) Lenovo Laptop (SN: R9-LDYVR 12/01)

4) Gray Dell Laptop (SN: 184CRF2)

5) HP Laptop (SN: CNU 1391T40)

6) Lenovo Tablet (SN : HGC89QYQ)

7) Blue HP Laptop (SN: TJ1805T1L6)

8) Galaxy S4 Phone (IMEI: 358011/05/023136/9)

9) SanDisk 32GB

10) SanDisk 128G

11) Silver HP Laptop (SN: CNU1402YY4)

12) Mini Computer

13) Black Gaming PC (SN: JY16070700240)

14) Black Amazon Tablet

15) Nvidia Shield (SN: 042301505098)

16) Seagate Hard Drive 3000GB (SN: Z500XYKK)

17) Seagate Constellation Hard Drive (SN: Z294CCDA)

18) Seagate Constellation Hard Drive (SN: Z2956FN5)

19) Western Digital 1 TB Hard Drive (SN: WCAU45363133)

20) Seagate Barracuda hard Drive (SN: WCASJ0826372)

21) Western Digital Hard Drive (SN: WCANKK977465)

22) Samsung Hard Drive (SN: S13UJ1KPC26424)

23) Pink BLU Phone (SN: 1110009016022953)

24) Black Samsung Galaxy S7 Phone (IMEI: 359755071452227)

25) Samsung SMG550T Phone (IMEI: 358511073771267)

26) Micro SD Card 16 GB

27) White iPhone 4

28) Black case with CDs

29) USB 8GB

30) PNY USB 32 GB

31) Dane-Elec USB 2GB

32) SMART Compact Flash

33) Transcend SD 32GB

34) Lexar SD 16GB

35) SanDisk Micro SD

36) Kingston Mini SD 1 GB

37) First title USB

38) Homemade Computer Tower

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

a. Any and all images of suspected child pornography and files containing images of suspected child pornography, any and all images believed to be an attempt to produce child pornography, in any form wherever it may be stored or found including, but not limited to:

   i. originals, thumbnails, and copies of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

   ii. videos (AKA motion pictures, films, film negatives), and other recordings or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

   iii. Images self-produced of the defendant and minors, and attempts to take or produce such;

   iv. Images of children, nude or otherwise, possessed, sent, received, or via message, email, or otherwise stored on the phone

   v. Internet history, including CACHE memory related to internet searches for child pornography or websites that could pertain such.

b. information or correspondence pertaining to the solicitation of others for sexual activity involving minors, and any and all information, messages, etc related to the sexual exploitation of children, including but not limited to:

   i. correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, text messages, establishing possession, identity of individuals, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

   ii. records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. Any and all address lists, names, contact information of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; and/or any information evidencing contact or correspondence with minors or adults in whatever form.

iv. Any and all chat log, text messages, email, or any type of communication in any form that is related to the sexual exploitation of minors for sexual purposes or related to the production, distribution or possession of child pornography.

c. records evidencing ownership of the subject item, including in and all lists of names, telephone numbers, addresses and contacts, and the content of voice mails and text messages and internet based applications, and internet or purchase history for any and all sexual devices, including but not limited to dildos, vibrators and sexual games.

d. Any and all security devices, to include encryption devices, needed to gain access to the devices;

e. Any and all address lists, names, contact information of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; and/or any information evidencing contact or correspondence with minors or adults in whatever form.

f. Any and all recordings, including those made by the defendant or the minor victim, or anyone else that depicts the defendant or others engaging in sexually explicit conduct of any type.

g. In searching the data, the computer personnel may examine and copy all of the data contained in the subject item to view their precise contents and determine whether the data falls within the items to be seized. In addition, the examining personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized.

ATTACHMENT C

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS :
:
: **ss. AFFIDAVIT**
:
COUNTY OF BENTON

Affidavit in Support of Application for Search Warrant

I, Ivan A. Martinez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the seizure and examination of property—electronic devices—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the U.S. Department of Justice Office of the Inspector General (OIG), currently assigned to the Dallas, Texas Field Office. I have been employed as a federal agent for approximately nineteen years. As part of my duties as an OIG Agent, I have investigated various crimes, to include crimes against children. These investigations have included the use of surveillance techniques, undercover activities, the interviewing of subjects and witnesses, and the planning and execution of search, arrest, and seizure warrants. I have participated in investigations involving persons who collect and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training in child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have conducted

criminal investigations involving the people who trade and exchange images of child sexual exploitation images between one another to reduce the risk of being apprehended by law enforcement. I have also discussed and reviewed these materials with other law enforcement officers. I have received on the job training, training at the Federal Law Enforcement Training Center (FLETC) and the U.S. Postal Inspection Service Training Academy.

3. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I am submitting this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant to seize and examine digital devices and other electronic storage media, also referred to as "SUBJECT ITEMS" (more fully specified in Attachment A). On August 1, 2019, the SUBJECT ITEMS were seized from the residence located at 17980 Crestwood Drive, Siloam Springs, Arkansas and from the person of Jon Jason Anderson, pursuant to a search warrant issued on July 31, 2019, by the Honorable Robin Green, Circuit Judge for Benton County, Arkansas. This warrant authorizes the seizure of the SUBJECT ITEMS, now being stored as evidence at the Benton County, Arkansas Sheriff's Office, Bentonville, Arkansas, and authorizes a forensic examination of those digital devices (SUBJECT ITEMS), for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(1), (a)(2) and (a)(4).

STATUTORY AUTHORITY

5. Title 18, United States Code, Section 2252(a)(1) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails,

any visual depiction if (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct. Title 18, United States Code, Section 2252(a)(2) prohibits a person from knowingly receiving, or distributing any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, . . . if (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct. Title 18, United States Code, Section 2252(a)(4) prohibits a person from knowingly possessing or accessing with intent to view a matter which contain[s] any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce . . . by any means including by computer if (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct.

6. "Child Pornography" is defined in Title 18, United States Code, Section 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

7. Title 18, United States Code, Section 2256(2)(A) defines "sexually explicit conduct" to mean actual or simulated (i) sexual intercourse, including genital-genital, oral-

genital, anal-genital, or oral-anal, whether between persons of the same sex or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person.

PROBABLE CAUSE

8. On or about May 6, 2019, Benton County Sheriff's Office (BCSO), Cyber Crimes Division, Sergeant Olin Rankin reviewed data from law enforcement Freenet computers which indicated that between February 23, 2019 and February 25, 2019, a computer running Freenet software with an Internet Protocol (IP) address of 70.178.159.118, and a Freenet Location ID of 0.882971054508456, requested blocks of suspected child pornography (CP) files containing hash values known by law enforcement databases to be associated with CP. Rankin noted that the user attempted to download more than one file associated with CP during that time-frame. Rankin utilized specially designated computers in the BCSO computer lab and validated that the files requested by the suspect, which included the following, depicted children engaged in sexual activity or poses in sexual manners.

9. On the same date, BSCO investigators utilized the law enforcement database Maxmind to conduct a query for IP address 70.178.159.118. The query indicated that the IP address was provided by Cox Communications and was believed to be operating in the location of Siloam Springs, Arkansas. BCSO investigators issued a subpoena to Cox Communications for IP address 70.178.159.118 which reported the account holder as Jon Jason "ANDERSON", residing at XXXXX Crestwood Drive, Siloam Springs, Arkansas, telephone number (479) 220-XXXX. Further inquiry of records into the address indicated that the residence was purchased in 2017 by ANDERSON and M.A.

10. On the afternoon of July 31, 2019, Rankin and BCSO Cyber Crimes Detective Alison Nguyen traveled to the residence located at XXXXX Crestwood Drive, Siloam Springs, Arkansas for further investigation. Investigators knocked on the front door, which was answered by ANDERSON, who was informed of the BCSO investigation into the IP address which they identified as his. Investigators requested ANDERSON's consent to a search of his devices for CP at which time ANDERSON invited them inside the residence and led them downstairs to a computer lab, which housed multiple computers and electronic devices. Prior to initiating their search, investigators provided ANDERSON a written BCSO "Consent to Search Computer Equipment/Electronic Data" form which ANDERSON signed consenting to a warrantless search of the electronic devices located inside of his residence.

11. Rankin located a computer, identified by ANDERSON as his, and conducted a search of the computer's electronic files and located and observed ten to twelve images of what Rankin, based on his training and experience, believed to be CP images of under aged children between the ages of eight and fourteen years of age. A description provided by Rankin of some of the images he viewed on ANDERSON's computer are as follows:

1b9ead31-903d-48c2-b756-f35295b8fb72_thumbcache_256.db.png
This image depicts a small child, approximately 8 – 10 years of age. The child appears to have semen in or on her vaginal area and is streaming down to her anus. In the foreground of the photo is an erect penis of an adult male. The focus of this image appears to be the vagina, semen and penis with the child's face in the background of the photo.

352ec0fd-58ff-4cc2-ace0-4099cea92f2f_thumbcache_256.db.png
This image appears to be a banner which has a young child depicted performing oral sex on an apparent adult male penis. There also appears to be a second image of a child lying down with semen near her vagina. The words "Hard Core Child Porn Archive" and "CP Image Archive" are displayed on the banner.

d754f2f8-4aa6-49b9-9d7c-d401e24e1eb5_thumbcache_256.db.png
This image depicts a nude child between the ages of 11 and 14 with her legs spread open exposing her vagina. There appears to be another subjects hand in the photograph holding an orange near the child. There is a small logo in the top left corner of the image.

12. Due to time of day and the high volume of electronic devices located inside the residence Rankin decided to obtain a State of Arkansas search warrant for ANDERSON's residence which would be executed the following day, on August 1, 2019.

13. Rankin informed ANDERSON and his wife, M.A. that they were not allowed back in the residence until the search was completed the following day. A uniformed BCSO deputy was dispatched to the residence and secured it through the night. At approximately 11:00 p.m. on the evening of July 31, ANDERSON called Rankin's cell phone and told Rankin that he did not want to put his family through the investigation and requested to meet with investigators for a voluntary interview.

14. On August 1, 2019, at approximately 12:08 a.m. ANDERSON traveled to the BCSO for a voluntary audio and video recorded interview with Nguyen. Prior to questioning, he was advised of his Miranda Rights from a written BCSO waiver of rights form which he signed and agreed to answer questions. ANDERSON said he was an "IT guy" and installed the Freenet software onto his computer in approximately 2018 to look for illegal pornography including bestiality. ANDERSON said that he used Freenet for mass downloading and just clicked through indexes for what he was searching for. ANDERSON explained that he did not have the intention of looking for a child, but for fifteen and sixteen year olds because he preferred flat breasts. Nguyen asked ANDERSON if he found fifteen and sixteen year olds and ANDERSON stated, "nothing that was satisfactory". ANDERSON told Nguyen he owned additional hard

drives that he used as "swap" drives for his computer that potentially had CP images on them. He told investigators they could locate the swap drives on the side of his home office.

15. On August 7, 2019, your Affiant and OIG Senior Special Agent Cloey Pierce traveled to the BCSO Jail where ANDERSON was in custody for alleged violations of State of Arkansas Computer Child Pornography Statute number A.C.A 5-27-603. ANDERSON agreed to a voluntary interview with OIG agents and signed a written OIG Warning and Waiver of Rights Form. ANDERSON told your Affiant that since approximately 2013 he worked as a contract computer network administrator. ANDERSON said he performed his duties remotely from his residence in Siloam Springs.

16. ANDERSON told your Affiant that in 2018 he downloaded the Freenet application software onto his personal laptop computer and used Freenet to access and download CP images of females ranging from the ages of fifteen to sixteen years of age. ANDERSON said he performed mass downloads through Freenet and afterwards selected images from the indexes that he was interested in. ANDERSON said that he was not interested in images depicting females under the fifteen or sixteen age range because he was turned off by those images. ANDERSON told your Affiant that he knew it was illegal to possess images of any under aged females and further admitted that he knew it was illegal to possess them at the time that he downloaded them.

17. The Devices are currently in storage at the Benton County Sheriff's Office located at 1300 SW 14th Street, Bentonville, Arkansas. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the BCSO.

TECHNICAL BACKGROUND

18. Based on my training, knowledge and experience, I am aware that individuals who commit online sexual exploitation offenses involving minors will often collect and/or view child pornography on their computer, and digital media storage devices, for several reasons:

a. They may receive sexual gratification and satisfaction, and/or fantasize about sexual contact with minors by viewing minors engaged in sexual activity or sexually suggestive poses;

b. They may collect sexually explicit or suggestive materials in a variety of media for their own sexual arousal and gratification;

c. They almost always possess and maintain their material in the privacy and security of their home or some other secure location. Child pornography distributors/collectors typically retain recordings, mailing lists, child erotica and store their child pornography amongst other, otherwise legal media or files. Digital evidence, like child pornography contraband, is different than traditional evidence that can be concealed, sold, used and/or destroyed and is not as volatile as other illegal items like narcotics; and

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by to enable the owner to view the collection, which is valued highly.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists

of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

19. Increasingly, individuals who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes, use mobile computing devices to do so. These portable devices can connect to the Internet at an individual's residence, or also through routers and wireless routers in various public and private locations. Mobile computing devices and electronic storage media such as laptops, tablets, smart phones, and flash drives, often travel with the person utilizing them and are commonly found in residences during search warrants.

20. I know computers serve four basic functions in connection with child pornography: production, communication, distribution and storage. Photographs and other digital images must be stored as data on a computer or other digital media device using specialized software to transfer images from a digital camera to a computer, or other electronic storage device, or by transferring images saved onto a media card to a computer or electronic storage device.

21. I know that if a child pornography viewer chooses to upgrade their electronic storage device, it is a simple process to transfer images from one device to another device. After the photograph or other image has been transferred onto the computer, the computer stores the data from the image as an individual "file." Such a file is generally known as a "GIF" (Graphic Interchange Format) or "JPEG" (for the Joint Photographic Experts Group, which wrote the

standard file, recognizable by the ".gif" or ".jpg" file extensions (hereinafter referred to as an "image file.)) Computers are capable of rendering the digital image on a computer screen, transferring the image to another computer, and/or printing the image.

22. I know that computer hardware, other digital devices, software, and electronic files are important to a criminal investigation in two distinct ways: the objects themselves may be contraband, evidence, instrumentalities, or fruits of a crime; and/or the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

23. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of electronic storage media (commonly referred to as a "hard drive") used on the home computers has grown tremendously within the last several years. Hard drives with the capacity of 160 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

24. I know from training and experience that computer systems commonly consist of computer processing units (CPU's) hard disks, hard disk drives, display screens, keyboards, printers, modems (used to communicate with other computers), electronic cables, USB flash drives, and other forms of magnetic and optical media containing computer information.

25. I know from training and experience that computers and magnetic and optical media are used to store information. In addition to the above-mentioned image files, that information often includes data files or other persons engaged in similar activities with minors, and lists of other exploited minors, as well as records of correspondence and conversations (printed or electronic) with such persons.

26. In addition to being evidence of a crime, there is probable cause to believe that the computers and their storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law. Accordingly, permission is sought herein to search computers and related devices consistent with the scope of the requested search.

27. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the Internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account

access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

28. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result, I believe that electronic evidence may be stored on any of the digital devices seized.

29. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

30. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they

are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic

evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

33. I submit that this Affidavit supports probable cause for a search warrant authorizing the seizure and examination of the SUBJECT ITEMS described in Attachment A to seek the items described in Attachment B as there is probable cause to believe that those items contain evidence of violations of Title 18, United States Code, Sections 2252(a)(1), (a)(2) and (a)(4).

Respectfully submitted,

Ivan Alejandro Martinez
Special Agent, DOJ/OIG

AFFIDAVIT subscribed and sworn to me this 19th day of September 2019.

Honorable Erin L. Wiedemann
Chief United States Magistrate Judge